

APPLICATION FOR UNITED STATES LETTERS PATENT

by

P. THOMAS WATSON

SCOTT R. SWIX

and

JAMES H. GRAY

for a

SET TOP BOX WITH FIREWALL

SHAW PITTMAN
1650 Tysons Boulevard
McLean, VA 22102-4859
(703) 770-7900
Attorney Docket Number: BS01-326

BACKGROUND

Field of the Invention

[0001] The present invention relates generally to a set top box.

Background of the Invention

[0002] Many dwellings including single homes, apartments, condominiums, town houses and lofts, have installed a media distribution system to improve the reception of audio and video content. Often, these distribution systems take the form of either a cable television system or a satellite television system. These systems receive a signal from a content supplier, such as a cable television company or a satellite television company. Generally, content suppliers offer a variety of services including different levels of subscriptions, pay channels and pay per view programs. Additionally, newer STBs, like Tivo, Replay TV and Ultimate TV, include computing resources including processors, hard disk drives, controllers, and operating systems.

[0003] STBs are often connected to various communications networks. In some cases, STBs are connected to the Internet via a telecommunications network. Although access to the Internet and telecommunications networks provides benefits to STBs, there are risks associated with this level of access.

[0004] One particular problem with permitting communication with telecommunications networks is the possibility that unauthorized users will gain access or send harmful messages to the STB. Viruses, commands, spam (excessive e-

mail) and other forms of unwanted communications have the potential to cause problems and interfere with the operation of a set top box.

SUMMARY OF THE INVENTION

[0005] The present invention is directed to a set top box that uses two ports to communicate with two respective communications networks. The first port communicates with the first network to receive programming information and the second port communicates with the second network to receive additional information including programming. The invention also includes a tuner capable of selecting a program and a firewall in communication with the second port and capable of receiving information from the second port. The firewall is capable of analyzing the information received from the second communications network. The firewall helps to prevent harmful or unauthorized information from reaching other components of the set top box.

[0006] In another aspect, the firewall receives communications from the second port before other components associated with the set top box.

[0007] In another aspect, the firewall is disposed logically between the second port and other components associated with the set top box.

[0008] In another aspect, the set top box further comprises a remote resource manager that is capable of receiving instructions from the second communications network.

[0009] In another aspect, the firewall includes packet filtering.

[0010] In another aspect, the firewall includes a proxy service.

[0011] In another aspect, the firewall includes stateful inspection.

[0012] In another aspect, the set top box further comprises a remote resource manager that is capable of receiving instructions from the second communications network.

[0013] In another aspect, the remote resource manager is capable of receiving an instruction from the second communications network and the instruction is used by the remote resource manager to modify the configuration of the set top box.

[0014] In another aspect, the remote resource manager is capable of sending information regarding resources associated with the set top box.

[0015] Additional features and advantages of the invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and advantages of the invention will be realized and attained by the structure and steps particularly pointed out in the written description, the claims and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] Figure 1 is a schematic diagram of a preferred embodiment of a system in accordance with the present invention.

[0017] Figure 2 is a schematic diagram of a preferred embodiment of a set top box in accordance with the present invention.

[0018] Figure 3 is a flow diagram of a preferred embodiment of a method in accordance with the present invention.

[0019] Figure 4 is a flow diagram of a preferred embodiment of a method in accordance with the present invention.

[0020] Figure 5 is a flow diagram of a preferred embodiment of a method in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0021] Figure 1 is a schematic diagram 100, portions of which show a preferred embodiment of the present invention. A service provider 102, which could be a network operator, is connected to network 104. Network 104 could be cable, terrestrial broadcast, satellite broadcast, or a combination of those forms. At least one STB 106 is connected to network 104. Usually, more than one STB 106 is connected to Network 104. However, for purposes of clarity, this description focuses on a single STB 106, keeping in mind that many more STBs could be connected to Network 104.

[0022] In addition to being connected to network 104, STB 106 is also preferably connected to a television 108. Preferably, service provider 102 distributes content through network 104 and STB 106 is adapted to receive that content and deliver it to television 108. In some embodiments, a residential gateway 114.

[0023] Residential gateway (RG) 114 is generally a device for terminating an external connection and fanning it out to multiple devices within a dwelling. In some embodiments, residential gateway 114 is a STB. Typically residential gateway 114 serves more than one purposes such as a DHCP server or as a NAT server for connections to the internet through an ISP. Residential gateway 114 can include storage, and in some cases residential gateway 114 is a managed device by the network provider.

[0024] In some cases, STB 106 includes a tuner that permits a user to access different programs or channels. In the preferred embodiment, STB 106 is connected to a second network 112. Typically, second network 112 is a telecommunications network and in some embodiments, second network 112 is a public switched telecommunications network ("PSTN"). Preferably, this second network 112 is capable of supporting Internet Protocol ("IP") communications. Preferably, network 112 supports two way communications between service provider 102 and STB 106. In some embodiments, second network 112 is a "broadband" network, for example, DSL, cable modem, Ethernet, or some other network that supports high speed communications. While the embodiment shown in Figure 1 shows STB 106 as a physically separate unit from associated television 108, it is possible to integrate an STB with a television. In such integrated units, the STB can be built into the television.

[0025] In some embodiments, STB 106 includes various resources that assist STB 106 in providing services to users. Referring to an embodiment of STB 106 shown in Figure 2. STB 106 can include several components including a fixed disk drive 202 that can be used to record content, and a second fixed disk drive 204 that could be used to provide increased storage capacity. A power supply 206 can be connected to a power source and to various components to provide power to those components. STB 106 can also include a first port 218, also referred to as a network port, capable of communicating with first network 104 (see Figure 1) and a second port 220, also referred to as a communications port, capable of communicating with second network 112 (see Figure 1).

[0026] STB 106 can also include a motherboard 208 that supports various other components. For example, in some embodiments, motherboard 208 can include a tuner 210 that can assist a user in selecting programs. A decoder 212 could be provided to assist in converting images from a digital format to a format suitable for display on a television. In one embodiment, decoder 212 is an MPEG-2 (Motion Picture Experts Group) decoder.

[0027] A remote resource manager (referred to as "RRM") 214 could also be associated with STB 106. In some embodiments, RRM 214 is attached to motherboard 208, in other embodiments, RRM 214 is a separate component that is located within or on STB 106 and RRM 214 is in communication with motherboard 208, and in other embodiments, RRM 214 is located outside STB 106 and is either attached or not attached to STB 106, and is in communication with motherboard 208.

[0028] RRM 214 is designed to determine resources that are associated with a particular STB. In the embodiment shown in Figure 2, RRM 214 is located within STB 106 and RRM 214 is designed to determine the resources associated with STB 106. In some embodiments, RRM 214 is designed to determine the resources that are associated with STB 106 at predetermined times, in other embodiments, RRM 214 determines the associated resources in response to a signal. Exactly when RRM 214 determines the nature and quality of the resources associated with STB 106 can be tailored to suit particular preferences and needs.

[0029] Some embodiments include an optional firewall 216. In some embodiments, firewall 216 is attached to motherboard 208. In some embodiments, firewall 216 is a software program that runs on STB 106. In other embodiments, firewall 216 is a

separate component that is located within or on STB 106 and is in communication with motherboard 208, and in other embodiments, firewall 216 is located outside STB 106 and is either attached or not attached to STB 106, and is in communication with motherboard 208.

[0030] Firewall 216 can be hardware, software or a combination of the two. Firewall 216 is designed to protect STB 106 from unauthorized access. Firewall 216 is in communication with communications port 218. In some embodiments, communications port 218 is a modular port, for example, an RJ-11 or an RJ-45. Since STB 106 is connected to a communications network 112 (see Figure 1) and because many different people have access to communications network 112, STB 106 may be vulnerable to unauthorized access or hacker attack.

[0031] To assist in preventing unauthorized access by third parties, firewall 216 is disposed logically between communications network 112 and other components of STB 106. In other words, firewall 216 receives information from communications network 112 before other elements of STB 106 and information from communications network 112 is sent to other components of STB 106 after firewall 216 has reviewed, analyzed, and or processed the information.

[0032] Firewall 216 can include filters, packet filtering, proxy service, and/or stateful inspection. Firewall 216 can process and/or analyze one or more communications protocols. Some examples of communications protocols that firewall 216 may be designed to process and/or analyze are: IP (Internet Protocol), TCP (Transport Control Protocol), HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message

Protocol), SMTP (Simple Mail Transport Protocol), SNMP (Simple Network Management Protocol), and/or Telnet.

[0033] Firewall 216 helps to stop and/or discourage outside influences such as “hackers” and “crackers” from gaining access to STB 106 and its components. For example, many of the new hacks to a STB for pirating programming is to have a replacement “smart” card and pirate software running in the STB. The pirate software periodically calls out using the STB modem to get updates of decryption keys. One way to counteract this attack is to change decryption keys so often that the pirate software can not call often enough to retrieve the latest keys since a dial up connection is relatively slow and a constant connection cannot be maintained. However, with a “broadband” connection like a DSL link and/or a Cable modem link that is generally “on at all times,” it is possible for the pirate software to keep up by a simple periodic access to a pirate web site for new decryption keys.

[0034] Firewall 216 can be used to counter even these new pirating methods. Firewall can be used to prevent access to STB 106 in the first place, and secondly, in some embodiments, firewall 216 can be used to prevent any unauthorized access to the Internet from within STB 106. For example, some piracy software programs including Trojan horse programs, automatically attempt to use the internet to retrieve information. Firewall 216 can be configured to prevent unauthorized access to the internet in general and/or to particular web sites.

[0035] The Figures 4 and 5 show flow diagrams of preferred embodiments of processes that can be used in conjunction with firewall 216 to prevent unauthorized access to and from STB 106.

[0036] Figure 4 is a flow diagram of a preferred embodiment of a process that can be used to prevent unauthorized entities and/or hackers from communicating with STB 106. In step 402, an outside entity attempts to communicate with STB 106. In steps 404 and 406, firewall 216 determines if the entity is authorized to communicate with STB 106 and determines if the communication protocol is an authorized. Both of these steps are optional, and none, one or both of the steps can be performed and in different order. If both the source and the protocol is acceptable, firewall 216 permits communication between the outside entity and STB 106. If either the source of the communication or the form of communication protocol or both are unacceptable, then firewall 216 forbids communication with STB 106. This occurs in step 410. After the decision has been made to either permit or deny communications between outside entity and STB 106, firewall 216 waits for the next communication in step 412.

[0037] Figure 5 is a flow diagram of a preferred embodiment of a process that can be used to prevent STB 106 from communicating with unauthorized web sites and/or other resources in communication with the internet. In step 502, STB 106 attempts to communicate with an outside entity. In steps 504 and 506, firewall 216 determines if STB 106 is authorized to communicate with the outside entity and determines if the communication protocol is an authorized. In one embodiment, firewall 216 determines if communications are permitted with the outside entity in question by using the target address of the outside entity. Both of these steps are optional, and none, one or both of the steps can be performed and in different order. If both the target address and the protocol is acceptable, firewall 216 permits communication between STB 106 and the outside entity. If either the target address or the form of

communication protocol or both are unacceptable, then firewall 216 forbids communication with the outside entity. This occurs in step 410. After the decision has been made to either permit or deny communications between STB 106 and the outside entity, firewall 216 waits for the next communication in step 412.

[0038] Figure 3 shows a flow diagram of a preferred embodiment of a method in accordance with the present invention. In Step 302, communication is initiated between service provider 102 and STB 106. Preferably this communications occurs over second network 112. As noted above, communication can be initiated in many different ways.

[0039] In one embodiment, communication is initiated by STB 106 at predefined intervals. For example, STB 106 initiates communications at a time when it is likely that users are not operating STB. In some embodiments, STB 106 initiates communications at 2:00 or 3:00 in the morning. STB 106 initiates communications by sending a signal over second network 112 to service provider 102. After receiving the signal, service provider 102 and STB 106 begin communications.

[0040] In other embodiments, service provider 102 initiates communications by sending the signal, preferably over second network 112, to STB 106. STB 106 responds to the signal from the service provider 102, and two-way communications between STB 106 and service provider 102 commences. In this embodiment, service provider 102 can initiate communications at predetermined times or service provider 102 can initiate communications manually by having technicians or operators associated with service provider 102 initiating communications.

[0041] After communications has been initiated, service provider 102 retrieves data from STB 106 in Step 304. Preferably, RRM 110 participates in the transmission of data to service provider 102. In one embodiment, RRM 110 receives a signal from service provider 102 and in response to that signal, RRM 110 retrieves data related to the various resources associated with STB 106.

[0042] This data can include information related to the resources associated with STB 106. This information could include the number, nature, type, kind and/or quality of components connected to or associated with STB 106 as well as the capabilities of those components. For example, in one embodiment, STB 106 uses RRM 110 to send information to service provider 102 regarding the number and size of all of the fixed disk drives that are associated with STB 106. RRM 110 can send the information automatically or in response to a second signal or request from service provider 102.

[0043] In Step 306, service provider 102 analyzes the data received from STB 106. In some embodiments, service provider 102 has access to a database or other storage facility that contains information related to STB 106. The information contained in the database relates to the configuration that service provider 102 expects of STB 106. For example, if the user of STB 106 has paid for a specific level of content and a specific size of an associated fixed disk drive 202, this information would be recorded in the database. For example, if user of STB 106 paid for basic subscription content plus a 10 gigabyte fixed disk drive, that information would be captured and recorded in the database.

[0044] Once the information related to the resources associated with STB 106 is received from STB 106, that information is compared with the information in the database. All differences between the information received from STB 106 and information retrieved from the database are noted.

[0045] For example, if the user has installed another fixed disk drive 204, or has changed the first fixed disk drive 202 to a different capacity fixed disk drive, and none of these modifications were authorized by service provider 102, service provider 102 can detect such unauthorized modifications in Step 306 where service provider 102 analyzes data from STB 106.

[0046] In step 308, data is sent from service provider 102 to STB 106. This is an optional step and need not be preformed. However, in some embodiments data could be sent to STB 106 that relates to programming content or information related to future programs. This can assist the user of STB 106 in selecting future programming for viewing and/or recording.

[0047] In some cases, service provider 102 will send operating instructions to STB 106. In those cases where service provider 102 sends operating instructions to STB 106, the service provider 102 has detected an unauthorized resource on STB 106 or service provider 102 would like to modify the configuration of STB 106.

[0048] In step 308, service provider 102 can send information and operating instructions to STB 106 to reconfigure STB 106 in such a way that the modified STB 106 will again conform to the expected configuration in accordance with the data retrieved from the database. Unauthorized modifications are generally rare, and therefore, these operating instructions are generally infrequently sent to STB 106.

[0049] In Step 310, STB 106 determines if an operating instruction has been sent from the service provider. If an operating instruction has been sent from the service provider 102, then STB 106 performs the operating instruction in Step 312. The operating instruction can include instructions that tell STB 106 to modify, disable, fail to address, or fail to use unauthorized resources. In addition, the operating command can also be used to allow or enable additional services, for example, permitting addressing of more HD space for extending record times or allowing extended EPG data, or allocate resources for new services, for example, electronic magazine or games, and/or repartitioning the fixed disk drive for more or less space for PVR or other services.

[0050] Continuing with the example, if the expected resource is a 10-gigabyte hard drive, and the user of STB 106 has installed a 20-gigabyte hard drive without authorization, STB 106 would receive an instruction to either disable the 20-gigabyte hard drive or instruct STB 106 to only access 10-gigabytes of the new fixed disk drive.

[0051] In some cases, users purchase STBs with more resources than they have initially paid, and as they pay additional money to service provider 102, service provider 102 enables those additional resources already associated with STB 106. In those cases where users have purchased an STB with more capabilities than their subscription level, the operating instruction would instruct STB 106 to use existing resources that it was previously not authorize to use.

[0052] For example, a service provider 102 could sell all of their STBs with large hard drives for example, a 200 gigabyte hard drive, and only permit access to certain

portions depending on the level of subscription payment. As users pay additional money, they are permitted to access greater and greater portions of their fixed disk drives. An operating instruction from service provider 102 can permit STB 106 to access additional portions of the fixed disk drive.

[0053] The operating instructions could be used to instruct STB 106 to receive or decode additional content. This feature could permit a service provider 102 to increase or decrease the level of content or the amount of content that STB 106 is authorized to receive. The operating instructions could also include information related to decrypting keys. By sending certain decrypting keys to STB 106, service provider 102 can control which programs STB 106 can successfully decode and consequently which programs the user of STB 106 can view.

[0054] In addition, the operating instructions can be used to determine if additional resources are available, for example, if additional fixed disk resources are available or if the correct processor to support MPEG 4 and/or MPEG 7 decoding in hardware or software is present. The operating instruction could also be used to diagnose software or hardware on an interactive basis with a technician from a remote location.

[0055] After the operating instructions have been performed in Step 312, an optional confirmation Step 314 can be performed. In this optional confirmation step, service provider 102 can retrieve information from STB 106 after STB 106 has been instructed to perform the operating instruction. In the confirm modification Step 314, service provider 102 can interrogate STB 106 after the operating instruction has been sent and retrieve information a second time and retrieve the information related to the new configuration, or the resources associated with STB 106. This information could

be compared with an expected configuration, thus permitting service provider 102 to determine if the operating instruction was successfully executed by STB 106.

[0056] In this way, service provider 102 can confirm whether the modification has been made or not. If the modification was not made, service provider 102 can retransmit the operating instructions to STB 106 or take other corrective action. If the modification has been successful and an appropriate response has been received from STB 106, the process moves to Step 316 where the system waits for the next communications with the STB to occur.

[0057] After communications are initiated at the next appropriate interval, the process then moves to Step 302. Using this preferred method, service provider 102 can determine the amount of resources associated with an STB 106, compare those resources with expected resources, and take any necessary corrective action.

[0058] The foregoing disclosure of the preferred embodiments of the present invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many variations and modifications of the embodiments described herein will be obvious to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claims appended hereto, and by their equivalents.

[0059] Further, in describing representative embodiments of the present invention, the specification may have presented the method and/or process of the present invention as a particular sequence of steps. However, to the extent that the method or process does not rely on the particular order of steps set forth herein, the method or

process should not be limited to the particular sequence of steps described. As one of ordinary skill in the art would appreciate, other sequences of steps may be possible. Therefore, the particular order of the steps set forth in the specification should not be construed as limitations on the claims. In addition, the claims directed to the method and/or process of the present invention should not be limited to the performance of their steps in the order written, and one skilled in the art can readily appreciate that the sequences may be varied and still remain within the spirit and scope of the present invention.